REMARKS

The Office Action of April 7, 2009 and the cited references have been carefully studied. Claims 47-73 are pending in the present application. The current claims define patentable subject matter and should be allowed. Favorable reconsideration is respectfully requested.

Claims 47-49, 51-54, 56-61, and 63-73 have been amended. Support for the amendments at least can be found in the specification. For example, on page 13, lines 16-28, the specification recites: "... It is noted that the storage device 205 illustrated in Fig. 2 is in direct connection with the analyzer 202, therefore it is included in the network information collector 201. Alternatively, it is appreciated that the storage device can be coupled by any other known method. For example, the storage device can be a networked database coupled to the analyzer via the Internet or it can be part of the analyzer 202. In other embodiments the storage device 205 can also be coupled to the network detector 203 and/or to the query engine 204 instead of or in addition to being coupled to the analyzer. Thus, the storage device 205 can be external to the network information collector 201 or located remotely therefrom, and it is therefore considered as associated therewith. In addition, it should be realized that the storage device can be, for example, a disk, a memory device (such as RAM), a RAID (Redundant Array of Independent, or Inexpensive Disks) or any other available device that can be used for storage of data..." (Emphasis added). As such, no new matter is added.

Other amendments to the form of the claims have also been made to the claims. Applicant respectfully submit that the amendments are purely ones of form and do not, nor are

they intended to, narrow the scope of the claims. Withdrawal of this objection is thus in order and respectfully requested.

Applicants respectfully note from the Office Action Summary at paragraph 10 that the drawings have been accepted by the Examiner.

Applicants also note with appreciation the Examiner's acknowledgement that the November 6, 2006, and December 4, 2006, Information Disclosure Statements (IDS) have been received and considered by the U.S.P.T.O.

Claim Objections

Claims 48, 63, 64, and 68 have been objected on the basis of informalities. Applicant has amended the claims to address the issue raised by the examiner. The objection has therefore been overcome. Withdrawal of the objection is respectfully requested.

Claim Rejection under 35 U.S.C. §101

In item 1 of the Office Action, claims 47-63 have been rejected under 35 U.S.C. §101 on the basis that the claimed invention is allegedly directed to non-statutory subject matter.

Claim 47 is an independent claim and claims 48-63 are dependent from claim 47. To advance prosecution, and without conceding the merits of the rejection, claim 47 has been amended to be tied to a computer readable medium, and thereby to comply with the structural/functional statutory requirement in MPEP 2106.01. Accordingly, the rejection has been overcome. Withdrawal of the rejection is respectfully requested.

Claim Rejection under 35 U.S.C. §102

In item 3 of the Office Action, claims 47-52, 57-58, 63-68, and 70-73 have been rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Publication No. 2003/0212910 ("Rowland et al."). Applicant respectfully traverses the rejection.

Claim 47 of the present application recites: "detecting, substantially in real-time, data conveyed by one or more detected nodes operating in the communication network in a manner that is transparent to said one or more detected nodes, giving rise to the detected data, thereby detecting said data passively;... querying at least one of one or more nodes operating in said communication network for said missing information provided at least partially from said storage device, giving rise to the queried nodes, thereby collecting said missing information actively." (Emphasis added.) These features are also somewhat similarly recited in independent claims 64 and 72-73, and are not disclosed or taught by Rowland et al.

According to the present application, a "smart" combination of passive and active network entities is provided, thereby enabling a substantially real-time inventory of all nodes (*e.g.*, representing a specific asset/device) within the communication network. This "smart" combination provides the ability to map all assets (connected to corresponding nodes) that operate within the network, and to maintain this information substantially in real-time. When a new node is provided into the network, it is detected passively (*e.g.*, page 14, line 15 to page 15, line 10); on the other hand, a node which is not transmitting anything is detected actively as well

as maintaining the "knowledge" that the node is still within the network, although no data is coming from it (*e.g.*, page 15, lines 5-10).

In addition, the communication network information is collected by means of a collector that consists of an analyzer coupled to a network detector, and to a query engine (page 13, lines 10-15). The network detector detects data conveyed by nodes operating in the communication network and operates in a manner that is transparent to the nodes and to the network, as recited in claim 47 of the present application. That is, according to an embodiment of the present application, the network detector does not convey data to nodes in the communication network; nor do the nodes convey data thereto. Thus, the network detector can operate passively in the communication network (page 14, line 15 to page 15, line 10). On the other hand, the query engine collects information relating to the network and/or to nodes therein by probing them. Thus, according to another embodiment of the present application, the network detector can operate actively in the communication network (page 15, lines 5-10). Further, being transparent to the network, the network detector relies on the network's activity in order to detect data conveyed by nodes operating therein. Unlike the query engine, the network detector is not required to transmit packets to nodes in the network in order to collect information relating thereto. The network detector detects data that is conveyed by the nodes as part of their communication scheme, as if the network detector does not exist. As such, it does not affect the performance of the network and the nodes (page 15, line 28-31).

Also, according to the present application, for each node within the communication network, a set of properties are collected in order to form a profile. Further, the system tracks the status of the network and the status of each node (*e.g.*, the system knows that a

node is now offline, or it is connected back to the network, or a number of changes have occurred within the network, etc.). This profile is generated based either on passive information and actively gathered information. According to an embodiment of the present application, the system for collecting information relating to a communication network is a learning system. It means that from the traffic being passively observed, the system detects the subnets against which it operates, detects which are the active elements operating on the network, and learns about any parameters, which can be trusted that is included within the observed network traffic (page 38, line 9-25), such as device IP (Internet Protocol) addresses, device operating system (OS) characteristics, and the like. Since not everything can be learned passively (*i.e.*, the topology related information), and since the passive detection can be dependent on user activity, the system actively compensates for these issues. The active compensation relates to querying for missing parameters both from the network and from assets/devices connected to nodes of said network. Also, the passively gathered information can be validated actively (*e.g.*, page 15, line 1 to page 16, line 4; page 33, line 1 to page 34, line 20). The queried nodes includes both nodes that send their traffic through the monitoring point, and also nodes, which exist on the network, but are not transmitting any traffic, or do not transmit any traffic through the monitoring point. For example, the system passively detects the subnets against which it is operating, and then starts passively detect the presence of corresponding devices; but, the system will search whether IP addresses, which are not detected per subnet, do represents "silent" nodes. Further, according to an embodiment of the present application, by combining between the passively and actively detected OS-related (Operating System) information a better OS detection solution is provided (page 23, line 19 to page 43).

Rowland et al. discloses a method and system for reducing the false alarm rate of a network intrusion detection system (NIDS). According to Rowland et al., the system receives alarms (events) from the NIDS and verifies whether the attacked operating system (OS) is operating on the attacked device by actively probing the attacked IP (Internet Protocol) address. This is done in order to reduce the amount of false alarms generated by the NIDS. The system of Rowland et al. does not have the understanding whether the attacked IP address is actually operating on the network. In addition, Rowland et al. does not teach passive deducing of any information from the network traffic (*i.e.*, learning characteristics of the device, performing passive OS detection, etc.), but rather Rowland et al. uses the NIDS to provide the disclosed system with non-contextual events (*i.e.*, an attack occurred against an IP address, and the like). Thus, according to Rowland et al., there is no knowledge regarding all elements operating on the network at any given time (Rowland et al., paragraph [0007]: "… A lower false alarm rate is facilitated even though knowledge of the entire protected network is not required…" etc.). Further, Rowland et al. also does not teach enabling passive observations at the traffic, when no alarm is received, and also, no information is received regarding the characteristics of all devices operating over the data network.

In addition, according to the present application, the network is queried for the missing information only when it is required. However, Rowland et al. teaches probing the network for the device OS related information always and in any circumstances upon receiving an alarm (*e.g.*, Abstract, page 2, paragraphs [0021-0023], etc.), since Rowland et al. does not teach deducing this information passively, when no alarm is received, and then identifying missing information, thus significantly reducing network traffic.

In summary, Rowland et al. neither discloses or teaches providing a "smart" combination of passive and active network sensors (thereby enabling having a substantially real-time inventory of all nodes within the communication network and providing the ability to map said all nodes, maintaining the substantially real-time information) nor combining between the passively and actively detected OS-related (Operating System) information to form a better OS detection solution. Therefore, Rowland at least does not disclose or teach the features of claims 47, 64, and 72-73 as recited above.

Accordingly, independent claims 47, 64, and 72-73 are patentable over Rowland et al., and claims 48-52, 57-58, 63, 65-68, and 70-71 are also patentable over Rowland et al. by virtue of their respectively dependency from claims 47 and 64, and inclusion of features recited therein. Withdrawal of this rejection is therefore respectfully requested.

Claim Rejections under 35 U.S.C. §103

In item 5 of the Office Action, claim 59 has been rejected under 35 U.S.C. §103(a) as being unpatentable over Rowland et al. in view of U.S. Patent Publication No. 2004/0078384 ("Keir et al."); in item 6 of the Office Action, claims 55-56 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Rowland in view of U.S. Patent No. 5,821,937 ("Tonelli et al."); in item 7 of the Office Action, claims 53-54, 60-62, and 69 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Rowland in view of U.S. Patent No. 7,089,306 ("Thorpe et al."). These rejections are respectfully traversed for the following reasons.

Keir et al. discloses a network vulnerability testing and reporting method and system including a selected combination of: (1) a non-destructive identification of target computer operating system; (2) a multiple-tier port scanning method for determination of what network addresses are active and what ports are active at those addresses; (3) a comparison of collected information about the target network with a database of known vulnerabilities; (4) a vulnerability assessment of some vulnerabilities on identified ports of identified target computers; (5) an active assessment of vulnerabilities reusing data discovered from previously discovered target computers; (6) an application of a quantitative score to objectively and comparatively rank the security of the target network; and (7) reduction of detailed results of the information collected into hierarchical, dynamic and graphical representations of the target network, target computers, and vulnerabilities found therein. However, Keir et al. does not teach providing a "smart" combination of passive and active network entities, thereby enabling having a substantially real-time inventory of all nodes within the communication network, and therefore does not make up for the deficiency of Rowland with respect to claims 47, 64, and 72-73 of present application.

Tonelli et al. discloses a software implemented method for auditing a network by using more than one soft probe to discover topology, host and interface information on devices in the network. According to Tonelli et al., the auditing includes gathering the data with soft probes that include a Simple Network Management Protocol (SNMP) probe and a Novell IPX probe. However, similarly to Rowland et al. and Keir et al., Tonelli et al. does not teach providing a "smart" combination of passive and active network entities, thereby enabling having a substantially real-time inventory of all nodes within the communication network, therefore does

not make up for the deficiency of Rowland with respect to claims 47, 64, and 72-73 of present application.

Thorpe et al. discloses a method and apparatus to collect information of different types that characterize a business entity and consolidate all these different types of information about the hardware, software and financial aspects of the entity in a single logical data store. The data store and the data collection system will have several characteristics that allow the overall system to scale well among the plethora of disparate data sources. However, similarly to the above cited references, Thorpe et al. does not teach providing a "smart" combination of passive and active network entities, thereby enabling having a substantially real-time inventory of all nodes within the communication network, therefore does not make up for the deficiency of Rowland with respect to claims 47, 64, and 72-73 of present application.

Accordingly, Applicant respectfully submits that claims 47, 64, and 72-73 are patentable over the cited references of record whether taken alone or in combination as proposed in the Office Action, claims 53-56, 59-62, and 69 are also patentable over the cited references by virtue of their dependency from claims 47 and 64, respectively, and inclusion of features recited therein. Withdrawal of these rejections is therefore respectfully requested.

Conclusion

In view of the above amendment and remarks, Applicant respectfully requests reconsideration and withdrawal of the outstanding rejections of record. Applicant submits that the application is in condition for allowance and early notice to this effect is most earnestly solicited.

If the Examiner has any questions, he is invited to contact the undersigned at 202-628-5197.

Respectfully submitted,

BROWDY AND NEIMARK, P.L.L.C.
Attorneys for Applicant(s)

By /Ronni S. Jillions/
Ronni S. Jillions
Registration No. 31,979

RSJ:HL
Telephone No.: (202) 628-5197
Facsimile No.: (202) 737-3528
G:\BN\C\cohn\Arkin2\Pto\2009-09-08Amendment.doc